

ESET Studie

Digitale Souveränität in Österreich

funktioniert nur mit
IT-Sicherheit „Made in EU“



Inhaltsverzeichnis

| | |
|--|----|
| Zwischen Geopolitik und Cybergefahren: Herausforderungen für Österreichs Wirtschaft | 3 |
| Was bedeutet „Made in EU“ überhaupt? | 4 |
| Über die Umfrage | 5 |
| Kernfragen..... | 5 |
| Welchen Sinn ergibt es, europäische Lösungen einzusetzen? | 10 |
| Digitale Souveränität ist ohne IT-Sicherheit „Made in EU“ unmöglich | 11 |
| Das spricht für „Made in EU“ | 12 |
| So hilft ESET Unternehmen bei der IT-Sicherheit | 13 |
| IT-Sicherheit auf dem Stand der Technik, „Made in EU“ | 14 |
| ESET bietet Informationssicherheit für Unternehmen jeder Größe | 17 |
| Fazit..... | 18 |
| Über ESET | 19 |



Cybersecurity
Progress. Protected.

Zwischen Geopolitik und Cybergefahren: Herausforderungen für Österreichs Wirtschaft

„Mögest Du in interessanten Zeiten leben“: So lautet eine dem chinesischen Kulturkreis zugeschriebene Verwünschung. Und ob wir es wollen oder nicht, wir leben genau in solchen Zeiten, angefangen bei den geopolitischen Anspannungen der jüngsten Vergangenheit. Der russische Angriffskrieg in der Ukraine, das dynamische Verhältnis mit den USA und nicht zuletzt eine wechselhafte wirtschaftliche Lage¹ lassen eine Frage aufkommen:

Wie reagieren Europa und Österreich auf diese Veränderungen?

Im Gegensatz zu anderen Regionen und Nationen liegen die Stärken der Europäischen Union und Österreichs nicht in natürlichen Ressourcen. Technologische Raffinesse im Einklang mit einem starken Wertekodex sind die Attribute, durch die sich die EU mit ihren Mitgliedern von anderen Regionen unterscheidet.

Allerdings stehen diese Werte und die österreichische Wirtschaft unter digitalem Dauerfeuer: Laut Studien sind drei von vier Unternehmen von Cyberangriffen betroffen. Gut jede vierte Attacke ist staatlich finanziert und stammt größtenteils außerhalb der EU. Der Schaden, der der österreichischen Wirtschaft allein durch Cyberangriffe in 2024 entstanden ist, belief sich auf 1,3 Milliarden Euro.

Diese Bedrohungen kommen aus unterschiedlichen Regionen mit verschiedenen Zielen: Vor allem zu China und Russland gehörende Hackergruppen haben es auf Organisationen in Europa abgesehen. Sie nehmen insbesondere Regierungsorganisationen sowie Transport- und Verteidigungsunternehmen ins Visier.

Diese beiden Faktoren – eine äußerst dynamische geopolitische Situation und eine wachsende Cyberbedrohungslage – lassen die Rufe nach mehr europäischer Souveränität lauter werden. Dazu gehört insbesondere eine starke IT-Sicherheit „Made in EU“.

¹ Quelle: <https://www.wifo.ac.at/publication/423473/>

„Auch österreichische Unternehmen sind vor globalen Veränderungen nicht gefeit. Viele haben erkannt, dass die Kombination aus hervorragender IT-Sicherheit und zuverlässigem Datenschutz nur bei europäischen Herstellern gegeben ist“,

— Matthias Malcher, Senior Territory Manager Austria bei ESET Deutschland GmbH



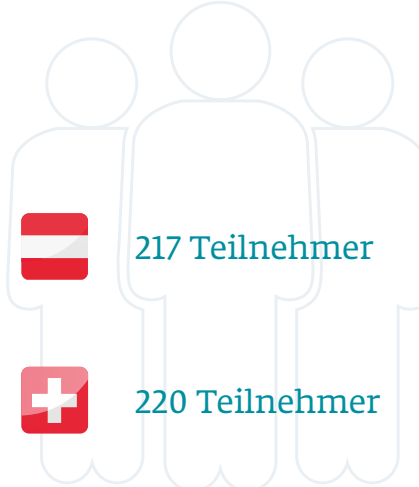
Was bedeutet „Made in EU“ überhaupt?



„Made in EU“ steht für Qualität, Sicherheit, Nachhaltigkeit und Vertrauen. Das Gütesiegel signalisiert, dass ein Produkt unter fairen Arbeitsbedingungen, nach der hiesigen Gesetzeslage und nach europäischen Qualitätsrichtlinien gefertigt wurde. Besonders in Zeiten wachsender Sensibilität für ethische Herstellung und kurze Lieferketten schafft „Made in EU“ Vertrauen und dient als starkes Kaufargument – vor allem im Vergleich zu Produkten aus Regionen mit weniger transparenten Standards.

Doch wie nehmen Unternehmen die Vorteile und Herausforderungen von IT-Sicherheit „Made in EU“ konkret wahr? Wem vertrauen österreichische IT-Entscheider noch und welche Rolle spielen europäische Werte? Um Antworten auf diese Fragen zu finden, hat ESET eine Umfrage unter österreichischen und Schweizer Unternehmensentscheidern durchgeführt. Diese Studie konzentriert sich auf die Ergebnisse aus Österreich.



437
Teilnehmer



 217 Teilnehmer
 220 Teilnehmer



Laufzeit von
27. Mai bis
02. Juni 2025

Über die Umfrage

Die vorliegende Studie wurde von der [techconsult GmbH](#) im Rahmen einer Online-Befragung durchgeführt. Sie beschäftigt sich mit der Herkunft aktuell eingesetzter sowie künftig geplanter IT-Sicherheitslösungen in Unternehmen. Befragt wurden insgesamt 437 Entscheider und IT-Entscheider aus Unternehmen aller Branchen und Größenklassen, davon 217 aus Österreich und 220 aus der Schweiz. Die Teilnehmer wurden gezielt vorselektiert, um eine valide Einschätzung aus Entscheiderperspektive zu gewährleisten. Die Erhebung erfolgte geschichtet nach Branchen und Unternehmensgrößen und ist repräsentativ für die jeweilige Grundgesamtheit.

Kernfragen

- Angesichts der aktuellen geopolitischen Entwicklungen – wie beurteilen Sie die Wahrscheinlichkeit, dass Sie die Herkunft Ihrer IT-Sicherheitslösungen überdenken oder diese sogar wechseln?
- Aus welcher Region würden Sie bevorzugt einen neuen Anbieter Ihrer zukünftigen IT-Sicherheitslösung wählen?
- Wie wichtig bzw. unwichtig ist die Herkunft des Herstellers bei der Auswahl von IT-Sicherheitslösungen für Ihr Unternehmen?
- Aus welcher Region stammt der Hauptanbieter Ihrer aktuellen IT-Sicherheitslösung?

Umfrage- ergebnisse



37%

der Unternehmen überdenken die Herkunft ihrer IT-Sicherheitslösung.

Die derzeitige geopolitische Lage beunruhigt viele Befragte. Viele Unternehmen befürchten offenbar, dass ihre IT-Sicherheitslösung im Ernstfall wirkungslos werden könnte. Das macht europäische Anbieter beliebter: Gut ein Drittel der Unternehmen denkt stark bis sehr stark über einen Wechsel der IT-Sicherheitslösung nach, 30 Prozent ziehen ihn

Frage 1: Angesichts der aktuellen geopolitischen Entwicklungen – wie beurteilen Sie die Wahrscheinlichkeit, dass Sie die Herkunft Ihrer IT-Sicherheitslösungen überdenken oder diese sogar wechseln?

Hypothese: Aufgrund der aktuellen Lage sind viele einem Wechsel der IT-Sicherheitslösung zugeneigt

Ergebnis: Bestätigt

mäßig in Erwägung. Am stärksten spielen größere Unternehmen ab 250 Mitarbeitern mit dem Gedanken umzusteigen. Gut jedes Dritte (36,7 %) tendiert stark bis sehr stark zu einem Wechsel seines Anbieters. Eine mögliche Erklärung hierfür: Große Unternehmen sind mutmaßlich von Datenschutzvorfällen und möglichen Betriebsstörungen stärker

betroffen als kleinere. Ein Wechsel zu einem anderen Anbieter, beispielsweise aus Europa, liegt deswegen nahe. Befragte aus dem Industriesektor hingegen ziehen einen Herstellerwechsel mäßig bis gar nicht in Betracht (93,2 %). Die Sorge ist hier wahrscheinlich, dass mit einem Herstellerwechsel ein Produktionsstillstand inklusive Umsatzeinbußen einhergeht.



61%

der befragten Wechselwilligen wollen zukünftig einen europäischen Anbieter beschäftigen.

Diejenigen Befragten, die wechselwillig sind, wollen mit großer Mehrheit einen IT-Sicherheitsanbieter aus der EU: Knapp zwei Drittel (61 %) geben an, zukünftig einen europäischen Anbieter wählen zu wollen. Gut jeder Fünfte (22,5 %) würde bei einem Wechsel einen US-amerikanischen Hersteller wählen. Diese Antworten zeigen: Europäische Lösungen genießen einen guten Ruf bei Öster-

Frage 2: Aus welcher Region würden Sie bevorzugt einen neuen Anbieter für Ihre zukünftige IT-Sicherheitslösung wählen?

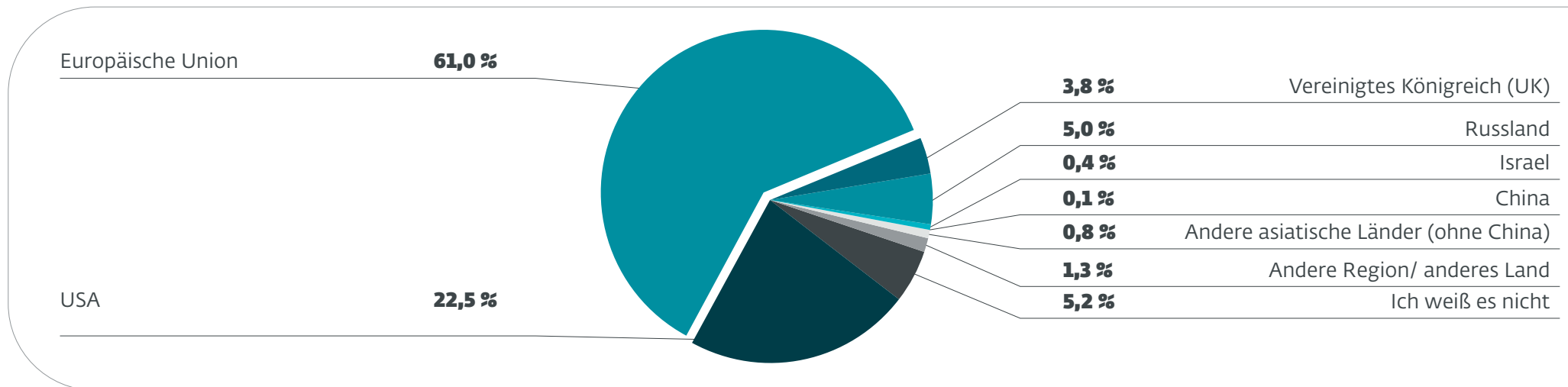
Hypothese: Europäische Lösungen sind erste Wahl bei Entscheidern.

Ergebnis: Teilweise bestätigt

reicher Unternehmensentscheidern. In Deutschland ist der Trend noch klarer, hier würden drei von vier Organisationen eine Lösung aus der EU wählen und nur 10 Prozent einen US-Hersteller.

In der österreichischen Industrie fällt diese Diskrepanz noch stärker auf: Hier würden über 80 Prozent einen US-Anbieter unter Vertrag nehmen.

Eine Erklärung hierfür ist, dass Industrieunternehmen aus Österreich eine starke globale Ausrichtung vorweisen, technologisch abhängig von etablierten US-Lösungen sind und europäische Datenschutz- und Souveränitätsaspekte im industriellen Kontext keine so große Rolle spielen wie in anderen Bereichen.



48%

der Befragten ist die Herkunft ihres IT-Sicherheitsanbieters wichtig

Österreichische Unternehmen legen generell hohen Wert auf die Herkunft ihres IT-Sicherheitsanbieters, wenn auch nicht so stark wie in Deutschland. Fast die Hälfte (48,4 %) gibt an, dass ihnen die Herkunft wichtig ist – in Deutschland sind es zwei

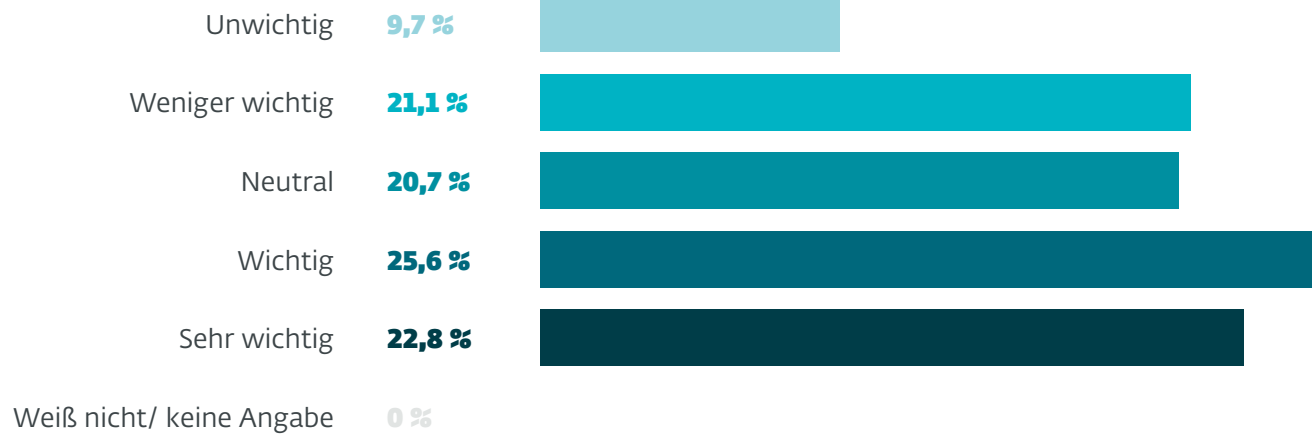
Frage 3: Wie wichtig bzw. unwichtig ist die Herkunft des Herstellers bei der Auswahl von IT-Sicherheitslösungen für Ihr Unternehmen?

Hypothese: Für die Mehrheit ist die Herkunft ein ausschlaggebendes Kriterium bei der Wahl einer IT-Sicherheitslösung

Ergebnis: Bestätigt

Drittel (67 %). Allerdings sind es auch hier wieder die großen Unternehmen ab 250 Mitarbeitern, die mehr Wert darauf legen: Fast 90 Prozent der Befragten ist die Herkunft wichtig. Dass für so viele Unternehmen die Ursprungsregion ihrer IT-Sicher-

heitslösung eine große Rolle spielt, liegt sicherlich an den hohen Datenschutzstandards, die hiesige Hersteller vorweisen können. Bei einem europäischen Anbieter müssen sie sich um Datenschutz und Compliance keine Sorgen machen.



38%

der Befragten nutzen bereits IT-Sicherheitsanbieter aus der EU

IT-Sicherheitslösungen aus der EU sind bei österreichischen Unternehmen beliebt: Mehr als ein Drittel (38,4 %) hat einen lokalen Anbieter in Verwendung, gut jeder Vierte (26,9 %) nutzt US-Hersteller. Andere Regionen wie das Vereinigte Königreich und China sind für Organisationen in Österreich nicht relevant.

Wieder fallen die österreichischen Industriebetriebe aus diesem Muster heraus: Hier nutzen mehr als drei

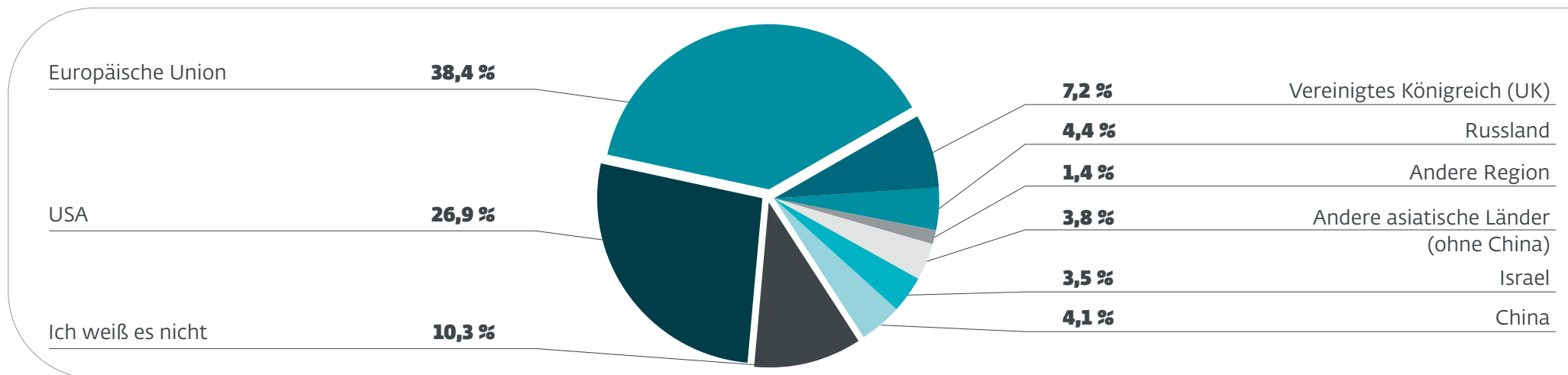
Frage 4: Aus welcher Region stammt der Hauptanbieter Ihrer aktuellen IT-Sicherheitslösung?

Hypothese: Österreichische Unternehmen vertrauen mehrheitlich auf europäische Lösungen.

Ergebnis: Mit Einschränkungen bestätigt

Viertel (77,6 %) der Befragten einen US-Hersteller. Eine mögliche Erklärung hierfür: Die Industrie hat langfristige Verträge mit US-Anbietern. Produktionsmaschinen und EDV-Systeme weisen in der Industrie häufig längere Nutzungszeiten auf als in anderen Wirtschaftszweigen, Verträge werden deswegen über längere Zeiträume geschlossen. Ein Herstellerwechsel in diesem Bereich ist zudem mit potenziellen Ausfallzeiten verbunden, die die wenigsten Betriebe

akzeptieren wollen. Gerade im Bereich der Operational Technology (OT) und bei Produktionsanlagen ist Kontinuität und Stabilität wichtiger als kurzfristige Innovation: Oberste Priorität hat die fortlaufende Produktion. Die Komplexität und Integrationsdichte der Systeme erschweren einen Umstieg zusätzlich. Eine Lösung, die einmal läuft, wird deswegen ungern gewechselt.



Interview

Welchen Sinn ergibt es, europäische Lösungen einzusetzen?



Dr. Jens Eckhardt ist Fachanwalt für Informationsrecht, Datenschutzauditor (TÜV) sowie IT-Compliance-Manager (TÜV) bei der Düsseldorfer Kanzlei pitc Legal Eckhardt Rechtsanwälte PartmbB. Im Gespräch mit Thorsten Urbanski, Director of Marketing bei ESET Deutschland GmbH, erklärt er, warum es in der IT-Sicherheit Sinn ergibt, auf „Made in EU“ zu setzen.

Thorsten Urbanski: Warum ist der Begriff „Made in EU“ im Cybersecurity-Kontext mehr als nur eine geografische Angabe?

Dr. Jens Eckhardt: In der Cybersicherheit geht es nicht nur darum, woher eine Lösung stammt – sondern vor allem darum, welchem Rechtsrahmen sie originär unterliegt. Ein Anbieter mit Sitz in der EU unterliegt denselben Gesetzen wie seine Kunden – etwa der DSGVO, dem zukünftigen BSI-Gesetz oder der NIS2-Richtlinie. Das schafft Vertrauen, rechtliche Klarheit und Verlässlichkeit, insbesondere im Haftungsfall.

Thorsten Urbanski: Gibt es aus juristischer Sicht konkrete Vorteile für Unternehmen, wenn sie auf europäische Anbieter setzen?

Dr. Jens Eckhardt: Ja. Zum einen vermeiden sie zusätzliche Hürden wie Drittland-Transfers nach DSGVO oder unklare Zugriffsbefugnisse ausländischer Behörden, die nicht durch den EU-Rechtsrahmen gebunden sind. Anbieter und Anwender bewegen sich im gleichen Rechtsrahmen. Das bedeutet: Ein möglicher Rechtsstreit

endet im Zweifel beim Europäischen Gerichtshof, dessen Entscheidungen beide Seiten unmittelbar binden. Das ist ein großer Vorteil gegenüber Anbietern aus außereuropäischen Rechtsordnungen.

Thorsten Urbanski: Was ändert sich durch die neue EU-Security-Regulation für die Unternehmensverantwortung – gerade mit Blick auf aktuelle Regulierungen wie NIS2?

Dr. Jens Eckhardt: Die Verantwortung der Geschäftsführung für IT-Sicherheit nimmt deutlich zu. Die NIS2-Richtlinie verpflichtet das Leitungsorgan explizit zur Billigung und Überwachung von „Cybersicherheitsmaßnahmen“. Gleichzeitig wird auch eine Schulungspflicht verankert. Das heißt: IT-Sicherheit ist kein technisches Randthema mehr, sondern eine zentrale Compliance- und Haftungsfrage auf Führungsebene.

Thorsten Urbanski: Wie lautet Ihr Fazit in Bezug auf die Frage, ob „Made in EU“ ein valides Auswahlkriterium für Cybersicherheitslösungen ist?

Dr. Jens Eckhardt: Absolut. Unternehmen profitieren von Rechtssicherheit, Nachvollziehbarkeit und politischen Stabilitätsvorteilen. In einer Welt zunehmender geopolitischer Spannungen bietet „Made in EU“ ein Maß an Vertrauen und Verlässlichkeit, das über technische Aspekte hinausgeht. Es ist eine strategische Entscheidung – sowohl für die Sicherheit als auch für die Unternehmensführung.

Digitale Souveränität ist ohne IT-Sicherheit „Made in EU“ unmöglich

Digitale Souveränität bedeutet die Fähigkeit Europas zur selbstbestimmten Nutzung, Entwicklung und Kontrolle digitaler Technologien und Infrastrukturen auf Basis europäischer Werte, Gesetze und Sicherheitsstandards. Sie setzt voraus, dass Staaten, Unternehmen und Institutionen unabhängig von außereuropäischen Anbietern agieren können, insbesondere im Bereich der IT-Sicherheit. Digitale Souveränität kann nur durch starke, vertrauenswürdige IT-Sicherheitslösungen „Made in EU“

gewährleistet werden. Der Ukraine-Konflikt zeigt eines deutlich: Eine staatliche Autonomie ist die Voraussetzung dafür, dass Wirtschaft, Gesundheitswesen und unsere Gesellschaft handlungsfähig sind und bleiben. Was einfach klingt, ist heute keinesfalls selbstverständlich. Denn überall dort, wo die IT-Security nicht auf höchstem Niveau und frei von politischen Restriktionen agiert, gerät die digitale Souveränität ins Straucheln.

„Gerade Industrieunternehmen in Österreich stehen vor der Herausforderung, ihre globalen Verflechtungen mit technologischer Souveränität in Einklang zu bringen. Europäische IT-Sicherheitslösungen bieten hier nicht nur erstklassige Technologie, sondern auch Rechtssicherheit und Datenschutz nach EU-Standards – ein strategischer Vorteil in Zeiten wachsender geopolitischer Spannungen und regulatorischer Anforderungen.“

— Matthias Malcher, Senior Territory Manager Austria bei ESET Deutschland GmbH

Das spricht für „Made in EU“

Mit der fortschreitenden Digitalisierung steigt der Komplexitätsgrad von IT-Systemen und IT-Infrastrukturen. Dadurch wird es für Unternehmen und Privatanwender immer schwieriger, einzelne IT-Sicherheitslösungen und deren Hintergründe zu verstehen und zu bewerten. Diese Entwicklung führt zu einer Verunsicherung der Menschen. Die Experten von ESET sensibilisieren unter dem Motto „IT-Sicherheit ist Vertrauenssache“ Organisationen wie Privatanwender zum Thema IT-Schutz Made in EU und engagieren sich für die Förderung der digitalen Souveränität. Seit über drei Jahrzehnten steht das Unternehmen für professionelle Schutztechnologien, die höchsten technischen, rechtlichen und ethischen Standards entsprechen.

Für diese Werte steht ESET als europäischer IT-Sicherheitshersteller:

- **Datenschutz und Compliance:** Als Unternehmen mit Hauptsitz in der EU ist ESET verpflichtet, die strengen Datenschutzstandards der Europäischen Union, einschließlich der DSGVO, zu erfüllen. Ihre Daten sind bei uns in sicheren Händen – das ist mehr als nur eine gesetzliche Regelung, der wir folgen, es ist eine Garantie, die wir allen Nutzern geben.
- **Vertrauenswürdigkeit und Transparenz:** Angesichts immer ausgeklügelterer Angriffe müssen Sie genau wissen, wem Sie Ihre Sicherheit anvertrauen. ESET steht für Transparenz, offene Kommunikation und eine klare Haltung gegen Backdoors und versteckte Zugänge. Ihre Sicherheit ist bei uns keine Frage des Vertrauens – es ist eine Frage der Überzeugung.

- **Geopolitische Stabilität:** In unserer vernetzten Welt kann die Wahl eines europäischen Anbieters den Unterschied ausmachen. ESET trägt zur digitalen Souveränität Europas bei und schützt kritische Infrastrukturen vor ungewollten externen Einflüssen. Sie stärken nicht nur Ihr Unternehmen, sondern auch die digitale Sicherheit Europas.

ESET war 2020 eines der ersten Unternehmen, das sich der TeleTrust-Initiative „IT Security Made in EU“ anschloss. Mit der Unterzeichnung der freiwilligen Konformitätserklärung setzen wir ein klares Zeichen für unser Engagement im Bereich Datenschutz und vertrauenswürdiger IT-Sicherheitstechnologien.

Als Mitglied der Initiative erfüllt ESET die fünf Kriterien, um das Siegel führen zu dürfen:

- ✓ Der Unternehmenshauptsitz ist in der EU
- ✓ Das Unternehmen bietet vertrauenswürdige IT-Sicherheitslösungen an
- ✓ „No Backdoor“-Garantie: Die angebotenen Produkte enthalten keine versteckten Zugänge
- ✓ Die IT-Sicherheitsforschung und -entwicklung findet in der Europäischen Union statt
- ✓ Das Unternehmen verpflichtet sich, den Anforderungen der EU-Datenschutz-Grundverordnung zu genügen





So hilft ESET Unternehmen bei der IT-Sicherheit

IT-Security Made in EU: Mehr als nur ein Label

Als europäischer Cybersicherheitsanbieter steht ESET seit über drei Jahrzehnten für professionelle Schutztechnologien, die höchsten technischen, rechtlichen und ethischen Standards entsprechen.

Datenschutz, Transparenz, offene Kommunikation und eine klare Haltung gegen Backdoors und versteckte Zugänge – wir von ESET entwickeln Schutz ohne Kompromisse.



Sicherheit ohne geopolitisches Risiko

Unsere Technologien entstehen in Europa. So trägt ESET zur digitalen Souveränität bei und schützt Wirtschaft, Behörden und Privatanwender vor ungewollten externen Einflüssen.



In Europa verwurzelt, weltweit im Einsatz

5 europäische Standorte mit starkem Netzwerk aus Partnern, Managed Service Providern und Distributoren, 8 Forschungs- & Entwicklungszentren in der EU und 100 % unabhängig.



Eigenes Rechenzentrum und Security Operations Center in Deutschland

Wer höchste Anforderungen an Datenschutz stellt, setzt auf unsere Rechenzentren und SOCs in Deutschland und der EU – mit Kerntechnologien, die lokal betrieben werden.



Ihre Daten bleiben in der EU

Wir von ESET kennen den gesetzlichen Rahmen, in denen sich unsere Kunden bewegen (müssen). Alle Daten werden innerhalb der EU gespeichert und verarbeitet, nach deutschem Datenschutzrecht und ohne Umwege über Drittstaaten.



Wir l(i)eben ein hohes Sicherheitsniveau

NIS2 und DSGVO: Als europäisches Unternehmen verstehen wir die EU-Regularien nicht nur, wir leben sie. Unser Team unterstützt unsere Kunden bei deren Umsetzung.



Eine No-Backdoor-Garantie ist für uns selbstverständlich – denn: Als IT-Sicherheitshersteller aus der EU stehen wir zu 100 % hinter den demokratischen Werten der europäischen Union.

— Holger Suhl, Country Manager DACH, ESET Deutschland GmbH

IT-Sicherheit ist Vertrauenssache

IT-Sicherheit auf dem Stand der Technik, „Made in EU“

Im Zuge der Umsetzung dieser Anforderungen an Unternehmen gewinnt auch das Qualitätssiegel „Made in EU“ zunehmend an Bedeutung: IT-Sicherheitslösungen aus der Europäischen Union stehen nicht nur für hohe technische Standards, sondern erfüllen in der Regel auch strenge Datenschutz- und Compliance-Vorgaben. Die Kombination aus technologischem Fortschritt und europäischen Werten stärkt das Vertrauen in die IT-Sicherheit und macht den „Stand der Technik“ zu einem strategischen Erfolgsfaktor für Unternehmen innerhalb der EU.

Darüber hinaus werden mit Inkrafttreten der NIS2-Richtlinie viele Unternehmen strengere Auflagen in ihrer IT-Sicherheit erfüllen müssen. Wie eingangs bereits erwähnt, ein Begriff, der in diesem Zusammenhang immer wieder fällt, ist der „Stand der Technik“. Dabei handelt es sich um einen

unbestimmten Rechtsbegriff: Der Gesetzgeber umgeht hiermit die Notwendigkeit, die Regelung ständig neu überarbeiten zu müssen, z. B. wenn sich ein Sachverhalt geändert oder die Technik weiterentwickelt hat. Die Sicherheit von Unternehmen muss sich dabei an zwei weiteren unbestimmten Rechtsbegriffen orientieren: dem Stand der Wissenschaft und Forschung sowie allgemein anerkannten Regeln der Technik.

Der Stand der Technik bezeichnet keine optionale Empfehlung, sondern eine verbindliche Anforderung, die sich aus Gesetzen wie der DSGVO oder der NIS2-Richtlinie ableitet. Für die IT-Sicherheit bedeutet das konkret: Organisationen müssen angemessene organisatorische und technische Maßnahmen treffen, um dem Stand der Technik zu entsprechen.

Mehr Informationen zum Thema „Stand der Technik“ lesen sie in diesem Whitepaper. [Jetzt herunterladen.](#)



Konkrete Handlungsempfehlungen

- **Vorbereitet sein:** Unternehmen sollten für den Worst Case einen Notfallplan in der Hinterhand haben, um den Betrieb aufrechtzuerhalten. Dazu gehört auch ein umfassendes Backup-Management, Wiederherstellungsmaßnahmen nach einem Notfall sowie eine passende Cyberversicherung.
- **Up-to-date sein:** Eine zentrale Management-Konsole hilft IT-Teams dabei, den Überblick zu den aktuellen (Versions-)Status von Clients, Servern und Mobilgeräten zu behalten. Außerdem können Updates hiermit automatisiert ausgerollt werden. Ein Patch & Vulnerability-Management erhöht die Sicherheit zusätzlich.
- **Datenhoheit behalten:** Datacenter sollten ausschließlich lokal oder in der EU liegen, um den höchstmöglichen Sicherheitsstandards zu entsprechen. So behalten Unternehmen die Kontrolle über ihre Daten.
- **Ausreichenden Datenschutz realisieren:** Personenbezogene Daten genießen seit Inkrafttreten der DSGVO einen besonderen Schutz. Unternehmen, die sie verarbeiten, müssen deshalb entsprechende Maßnahmen treffen, um sie vor unberechtigtem Zugriff zu bewahren. Dazu gehört beispielsweise eine sichere Verschlüsselung auf Endgeräten.

- **Budget einplanen:** Entscheider sollten für ihre Sicherheitslösungen Kosten einplanen. Auf diese Weise sinkt die Wahrscheinlichkeit für Produktionsausfälle und damit einhergehende Folgeschäden.
- **Vertrauen? Zero.** Zumindest im Sinne eines Zero-Trust-Modells. Das heißt, Mitarbeiter sollten nur Zugriff auf die Daten erhalten, die sie wirklich für ihre tägliche Arbeit benötigen. Solche Zero-Trust-Konzepte bieten zudem eine Orientierungshilfe, wie man das eigene Netzwerk unter Berücksichtigung individueller Anforderungen optimal schützen kann.

Besonders der letzte Punkt ist für die IT-Sicherheit von Organisationen sehr wichtig. Das Zero Trust-Konzept von ESET besteht aus einem dreistufigen, aufeinander aufbauenden Reifegradmodell. Je höher die Stufe ist, desto sicherer ist die Schutzwirkung – also „reifer“. Ob als Standardlösung oder Managed Service – die Kombination aus Endpoint Security, Verschlüsselung, Multi-Faktor-Authentifizierung, Cloud Sandboxing und Schutz für Cloud-Anwendungen bildet dabei das richtige Fundament für Zero Trust – nicht nur, um dem Stand der Technik zu entsprechen, sondern auch, um so gut wie möglich vor Cyberbedrohungen geschützt zu sein.

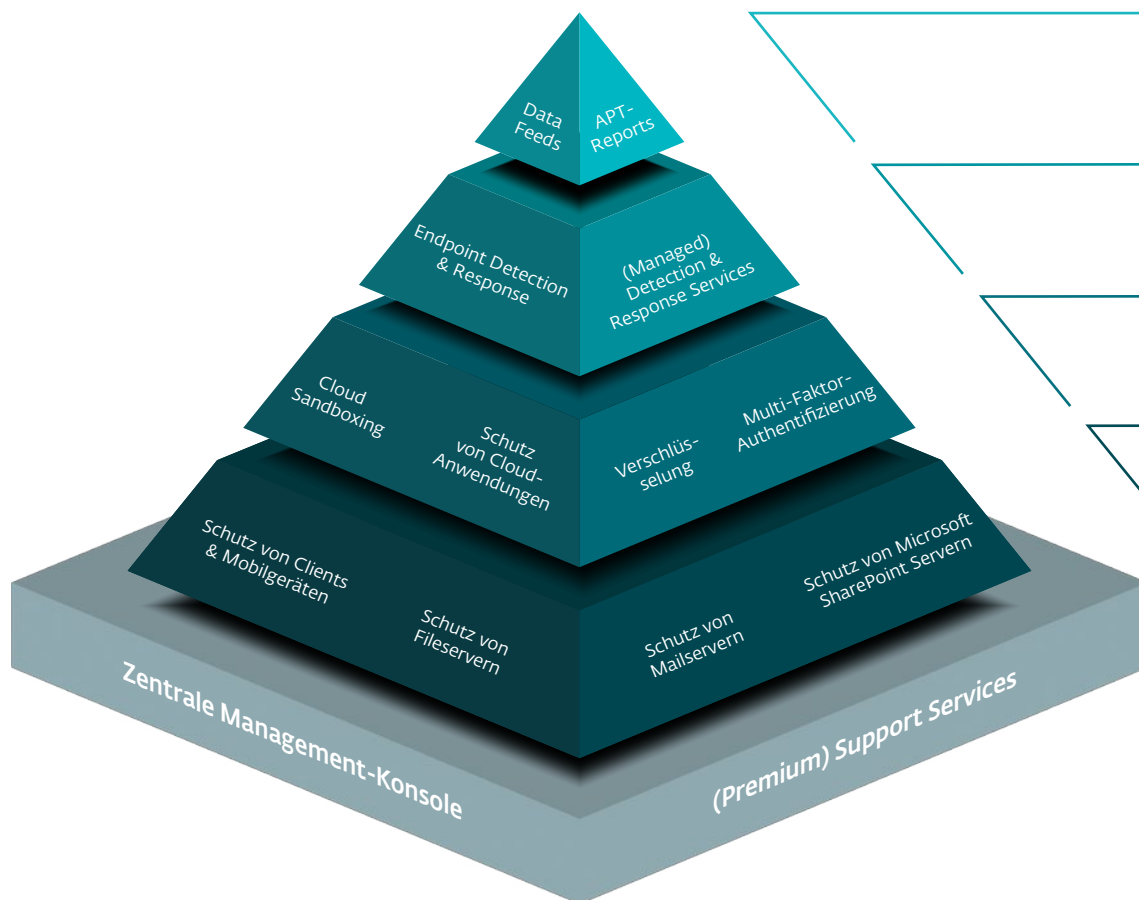


Eine aktuelle Umfrage von ESET bestätigt, wie wichtig das Zero-Trust-Konzept von ESET zur Verbesserung des Stands der Technik in Organisationen ist: Fast 95 Prozent geben an, dass das Modell ihnen beim Erreichen des Stands der Technik hilft. Allerdings ist laut eigener Aussage nur knapp jeder

Dritte (31 %) finanziell und personell gut aufgestellt – bei knapp 29 Prozent mangelt es trotz passender Finanzen und vorhandenem Personal an Qualifizierung bzw. Weiterbildungen. Hier besteht für die Zukunft noch Handlungsbedarf.

EINSATZBEREICH

SCHUTZLEVEL



GANZHEITLICHES LAGEBILD – AUSSENSICHT

Stufe 3: Bietet tiefe Einblicke in die globale Bedrohungslandschaft als Grundlage für einen SOC-/SIEM-Betrieb

GEFAHRENSUCHE UND ABWEHR – INNENSICHT

Stufe 2: Gewährleistet die Wirksamkeit der IT-Sicherheit mittels Anomalieerkennung, Schwachstellenanalyse und Incident Management

GRUNDSCHUTZ PLUS

Stufe 1: Empfohlene zusätzliche Absicherung für Cloud-Anwendungen, Daten und Zugänge sowie erweiterter Schutz vor Zero-Days

GRUNDSCHUTZ BASIS

Stufe 0: Mindestabsicherung für Endgeräte und Server

ESET bietet Informationssicherheit für Unternehmen jeder Größe

Qualitätsmanagement – Made in EU:

- Überall verfügbar – vollautomatischer Schutz der gesamten Organisation
- Volle Kontrolle über Ihre Daten dank transparenter (Sample-)Analysen innerhalb der EU
- Einzigartige Geschwindigkeit bei der Analyse von eingehenden Warnmeldungen
- Zuverlässig und sicher – alle Anforderungen von Datenschutzbestimmungen (bspw. DSGVO) bequem erfüllen
- Große Flexibilität in puncto Lizenzform, Hardwareeinsatz und Anforderungen an die Infrastruktur

Vorteile für Unternehmen:

- Passgenaue IT-Sicherheit für alle Unternehmensgrößen und -anforderungen
- Mitarbeiter entlasten und (Hardware-) Ressourcen schonen
- Compliance und Sicherheitsstandards erweitern
- Verwaltung der Schutzlösungen für alle gängigen Betriebssysteme via ESET PROTECT (Cloud oder On-Premises)
- Lizenzvielfalt – Kombination beliebiger Betriebssysteme (Windows, macOS, Linux) und Geräte (Clients, Server, Mobilgeräte) entsprechend der Bedürfnisse

„Als Security-Hersteller bieten wir moderne Lösungen, Dienstleistungen und Konzepte an, mit denen Unternehmen und Verwaltungen eine Cyber-Resilienz auf höchstem Niveau gestalten können.“

— Holger Suhl, Country Manager DACH,
ESET Deutschland GmbH



Fazit

Die aktuelle Studie zeigt, wie stark geopolitische Spannungen und zunehmende Cyberbedrohungen das Sicherheitsbewusstsein österreichischer Unternehmen verändern. Während europäische IT-Sicherheitslösungen vor allem im Hinblick auf Datenschutz, Rechtssicherheit und politische Stabilität punkten, zeigt sich insbesondere in der Industrie eine große Zurückhaltung gegenüber einem Wechsel von etablierten US-Anbietern. Langfristige Verträge, komplexe Systemlandschaften und der hohe Stellenwert von Betriebskontinuität erschweren hier den Umstieg.

Dennoch ist der Wunsch nach mehr digitaler Souveränität in Österreich deutlich spürbar – besonders bei größeren Unternehmen, die sich stärker mit regulatorischen Anforderungen wie der DSGVO oder der NIS2-Richtlinie konfrontiert sehen. IT-Sicherheit „Made in EU“ bietet ihnen entscheidende Vorteile: Sie erfüllt nicht nur höchste technische Standards, sondern garantiert auch eine klare rechtliche Grundlage ohne Drittlandrisiken. Europäische IT-Sicherheitsanbieter bieten gegenüber außereuropäischen Lösungen den Vorteil eines einheitlichen

und strengen Datenschutzrechts (insbesondere der DSGVO), klarer Haftungsregeln und einer transparenten Unternehmenspraxis – inklusive „No Backdoor“-Garantie. Gerade im Lichte der Erfahrungen mit kritischen Infrastrukturen in Kriegs- und Krisensituationen wird deutlich, wie schnell technische Systeme zu geopolitischen Spielbällen werden können.

Der europäische Ursprung wird dabei zunehmend als strategisches Auswahlkriterium verstanden – nicht zuletzt, weil Unternehmen sich durch ihn besser gegen geopolitische Einflussnahme und unerwünschte Zugriffe absichern können.

Die Untersuchung macht deutlich: Wer auch in Zukunft wettbewerbsfähig, rechtskonform und resilient bleiben will, sollte IT-Sicherheit als Führungsaufgabe begreifen – und europäische Lösungen ernsthaft in Betracht ziehen. Digitale Souveränität beginnt für österreichische Unternehmen mit der bewussten Wahl eines vertrauenswürdigen, transparenten und rechtssicheren Partners – am besten aus der EU.



Über ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Organisationsgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihre Infrastruktur mithilfe von Cloud Sandboxing frei von Zero-Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungslösungen unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen sowie Compliance-Maßnahmen.

Unsere Endpoint Detection and Response-Lösung, dedizierte Services wie z.B. Managed Detection and Response und Frühwarnsysteme in Form von Threat Intelligence ergänzen das Angebot im Hinblick auf Incident Management sowie den Schutz vor gezielter Cyberkriminalität und APTs. Dabei setzt ESET nicht allein auf modernste KI-Technologie, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

3 VON ÜBER 500.00 ZUFRIEDENEN KUNDEN



Seit 2019 ein starkes Team auf dem Platz und digital



Seit 2016 durch ESET geschützt
Mehr als 4.000 Postfächer



ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT



ESET wurde das Vertrauensiegel „IT Security made in EU“ verliehen



Unsere Lösungen sind nach den Qualitäts- und Informationssicherheitsstandards ISO 9001:2015 und ISO/IEC 27001:2013 zertifiziert

ESET IN ZAHLEN

110.000.000+

Geschützte Nutzer weltweit

500.000+

Geschützte Unternehmen

178

Länder & Regionen

11

Forschungs- und Entwicklungszentren weltweit



ESET Deutschland GmbH
Spitzweidenweg 32
07743 Jena
Tel.: +49 3641 3114 200